Modular equations for Lubin-Tate formal groups at chromatic level 2

YIFEI ZHU

We give an integral lift of the Kronecker congruence for moduli of finite subgroups of elliptic curves. This leads to a uniform presentation for the power operation structure on Morava E-theories of height 2.

55S25; 11F23, 11G18, 14L05, 55N20, 55N34, 55P43

1 Introduction

1.1 Moduli of elliptic curves and of formal groups

The Kronecker congruence

$$\big(\widetilde{j} - j^p\big)\big(\widetilde{j}^p - j\big) \equiv 0 \mod p \tag{1.1}$$

gives an equation for a curve that represents the moduli problem $[\Gamma_0(p)]$ for elliptic curves over a perfect field of characteristic p. This moduli problem associates to such an elliptic curve its finite flat subgroup schemes of rank p. A choice of such a subgroup scheme is equivalent to an isogeny from the elliptic curve with a prescribed kernel. The j-invariants of the source and target curves of this isogeny are parametrized by the coordinates j and $\widetilde{j}$.

More precisely, the Kronecker congruence provides a *local* description for $[\Gamma_0(p)]$ at a supersingular point. For large primes p, the supersingular locus at p may consist of more than one closed point. In this case, the modular curve does not have an equation in the simple form above; only its completion at a single supersingular point does.

Integrally, there are polynomials that describe the modular curve for $[\Gamma_0(p)]$ over $\operatorname{Spec}\mathbb{Z}$. The "classical modular polynomials" lift and globalize the Kronecker congruence, while the "canonical modular polynomials," in a different pair of parameters, appear simpler (see the Modular Polynomial Databases in Magma for the terminology and numerical examples). Computing these modular equations for $[\Gamma_0(p)]$ can be

difficult. As Milne warns in [Milne2012, Section 6], "one gets nowhere with brute force methods in this subject."

On a related subject, Lubin and Tate developed the deformation theory for one-dimensional formal groups of finite height [Lubin-Tate1966]. Later, with motivation from algebraic topology, Strickland studied the classification of finite subgroups of Lubin-Tate universal deformations. In particular, he proved a representability theorem for this moduli of deformations [Strickland1997, Theorem 42].

At height 2, there is a connection between the moduli of formal groups and the moduli of elliptic curves. This is the Serre-Tate theorem, which states that p-adically, the deformation theory of an elliptic curve is equivalent to the deformation theory of its p-divisible group [Lubin-Serre-Tate1964, Section 6]. In particular, the p-divisible group of a supersingular elliptic curve is formal.

Thus the local information provided by the Kronecker congruence (and its integral lifts) becomes useful for understanding deformations of formal groups of height 2. In this paper, we give an explicitation for the representing formal scheme in Strickland's theorem. Equivalently, this describes the complete local ring of $[\Gamma_0(p)]$ at a supersingular point, i.e., relative to the universal formal deformation of a supersingular elliptic curve in characteristic p, as studied by Katz and Mazur [Katz-Mazur1985].

Theorem 1.2 *Let $\mathbb{G}_0$ be a formal group over $\overline{\mathbb{F}}_p$ of height 2, and let $\mathbb{G}$ be its universal deformation. Write A_m for the ring $\mathcal{O}_{\mathrm{Sub}_m(\mathbb{G})}$ studied in [Strickland1997], which classifies degree-p^m subgroups of the formal group $\mathbb{G}$. In particular, write $A_0 \cong \mathbb{W}\big(\overline{\mathbb{F}}_p\big)[\![h]\!]$ according to the Lubin-Tate theorem.*

Then the ring $A_1 \cong \mathbb{W}\big(\overline{\mathbb{F}}_p\big)[\![h,\alpha]\!]/\big(w(h,\alpha)\big)$ is determined by the polynomial

$$w(h,\alpha) = (\alpha - p)\big(\alpha + (-1)^p\big)^p - \big(h - p^2 + (-1)^p\big)\alpha \tag{1.3}$$

which reduces to $\alpha(\alpha^p - h)$ modulo p.

Remark 1.4 As a result of a different choice of parameters, the last congruence above is not in the form of Kronecker's (cf. [Katz-Mazur1985, Remark 7.7.1] and see Section 2 below). In fact, let $\widetilde{\alpha}$ denote the image of α under the Atkin-Lehner involution, so that $\alpha \cdot \widetilde{\alpha} = (-1)^{p+1}p$, which is the constant term of (1.3) as a polynomial in α. Dividing a factor of α from the modular equation $w(h,\alpha) = 0$, we obtain a congruence

$$h \equiv \alpha^p + \widetilde{\alpha} \mod p$$

This is a manifest of the Eichler-Shimura relation $T_p \equiv F + V \mod p$ between the Hecke, Frobenius, and Verschiebung operators, which reinterprets $[\Gamma_0(p)]$ in characteristic p.

The polynomial $w(h,\alpha)$ can be viewed as a local variant of a canonical modular polynomial, whose parameters are the j-invariant and a certain eta-quotient. See [Choi2006, Example 2.4, esp. (2.4)] for an algorithm that we will adapt to prove Theorem 1.2 in Section 3 below. Related to this, compare the sequences $\{j_n^{(p)}(z)\}_{n=1}^{\infty}$ in [Ahlgren2003], with $p \in \{2,3,5,7,13\}$, and $\{j_m(z)\}_{m=0}^{\infty}$ in [Bruinier-Kohnen-Ono2004] of Hecke translates of Hauptmoduln, which explain the relation $h = T_p\,\alpha$ from above.

1.2 Algebras of cohomology operations

The Adem relations

$$\mathrm{Sq}^i\,\mathrm{Sq}^j = \sum_{k=0}^{[\frac{i}{2}]} \binom{j-k-1}{i-2k} \mathrm{Sq}^{i+j-k}\,\mathrm{Sq}^k \qquad 0<i<2j \tag{1.5}$$

describe the multiplication rule for the Steenrod squares Sq^i. These are power operations in ordinary cohomology with $\mathbb{Z}/2$-coefficients. In general, for ordinary cohomology with $\mathbb{Z}/p$-coefficients, the collection of its power operations has the structure of a Steenrod algebra.

Quillen's work connects complex cobordism and the theory of one-dimensional formal groups [Quillen1969]. From this viewpoint, ordinary cohomology theories with $\mathbb{Z}/p$-coefficients fit into a framework of chromatic homotopy theory, as theories concentrated at height ∞.

The power operation algebras for cohomology theories at other chromatic levels have been studied as well. In particular, key to the chromatic viewpoint is a family of Morava E-theories, one for each finite height n at a particular prime p. More precisely, given any formal group $\mathbb{G}_0$ of height n over a perfect field of characteristic p, there is a Morava E-theory associated to the Lubin-Tate universal deformation of $\mathbb{G}_0$. Via Bousfield localizations, these Morava E-theories determine the chromatic filtration of the stable homotopy category.

There is a connection between (stable) power operations in a Morava E-theory E and deformations of powers of Frobenius on its corresponding formal group $\mathbb{G}_0$. This is Rezk's theorem, built on the work of Ando, Hopkins, and Strickland [Ando1995, Strickland1997, Strickland1998, Ando-Hopkins-Strickland2004]. It gives an equivalence of categories between (i) graded commutative algebras over a Dyer-Lashof algebra for E and (ii) quasicoherent sheaves of graded commutative algebras over the moduli problem of deformations of $\mathbb{G}_0$ and Frobenius isogenies [Rezk2009, Theorem

B]. Here, the Dyer-Lashof algebra is a collection of power operations that governs all homotopy operations on commutative E-algebra spectra [Rezk2009, Theorem A].

At height 2, information from the moduli of elliptic curves allows a concrete understanding of the power operation structure on Morava E-theories. Rezk computed the first example of a presentation for an E-Dyer-Lashof algebra, in terms of explicit generators and quadratic relations analogous to the Adem relations (1.5) [Rezk2008]. Moreover, he gave a uniform presentation, which applies to E-theories at all primes p, for the mod-p reduction of their Dyer-Lashof algebras [Rezk2012, 4.8]. Underlying this presentation is the Kronecker congruence (1.1) [Rezk2012, Proposition 3.15].

In this paper, we provide an "integral lift" of Rezk's presentation, in the same sense that Theorem 1.2 above lifts the Kronecker congruence. We start with the following.

Theorem 1.6 *Let E be a Morava E-theory spectrum of height 2 at the prime p. There is a total power operation*

$$\begin{aligned}\psi^p \colon\ E^0 &\to E^0(B\Sigma_p)/I\\ \mathbb{W}\big(\overline{\mathbb{F}}_p\big)[\![h]\!] &\to \mathbb{W}\big(\overline{\mathbb{F}}_p\big)[\![h,\alpha]\!]/\big(w(h,\alpha)\big)\end{aligned}$$

where I is an ideal of transfers.

(i) *The polynomial*

$$w(h,\alpha) = w_{p+1}\alpha^{p+1} + \cdots + w_1\alpha + w_0 \qquad\qquad w_i \in E^0$$

can be given as (1.3) from Theorem 1.2. In particular, $w_{p+1} = 1$, $w_1 = -h$, $w_0 = (-1)^{p+1}p$, and the remaining coefficients

$$w_i = (-1)^{p\,(p-i+1)}\left[\binom{p}{i-1} + (-1)^{p+1}p\binom{p}{i}\right]$$

(ii) *The image $\psi^p(h) = \sum_{i=0}^{p} Q_i(h)\,\alpha^i$ is then given by*

$$\psi^p(h) = \alpha + \sum_{i=0}^{p}\alpha^i\sum_{\tau=1}^{p} w_{\tau+1}\,d_{i,\tau}$$

where

$$d_{i,\tau} = \sum_{n=0}^{\tau-1}(-1)^{\tau-n}\,w_0^n \sum_{\substack{m_1+\cdots+m_{\tau-n}=\tau+i\\ 1\le m_s\le m_{s+1}\le p+1}} w_{m_1}\cdots w_{m_{\tau-n}}$$

In particular, $Q_0(h) \equiv h^p \mod p$.

This leads to the following.

Theorem 1.7 *Continue with the notation in Theorem 1.6. Let Γ be the Dyer-Lashof algebra for E, in the sense of [Rezk2009], which is the ring of additive power operations on $K(2)$-local commutative E-algebras.*

Then Γ admits a presentation as the associative ring generated over $E^0 \cong \mathbb{W}\big(\overline{\mathbb{F}}_p\big)[\![h]\!]$ by elements Q_i, $0 \le i \le p$, subject to a set of relations.

(i) *Adem relations*

$$Q_k Q_0 = -\sum_{j=1}^{p-k} w_0^j\, Q_{k+j} Q_j - \sum_{j=1}^{p} \sum_{i=0}^{j-1} w_0^i\, d_{k,j-i}\, Q_i Q_j \qquad \text{for } 1 \le k \le p$$

where the first summation is vacuous if $k = p$.

(ii) *Commutation relations*

$$Q_i\, c = (Fc)\, Q_i \quad \text{for } c \in \mathbb{W}\big(\overline{\mathbb{F}}_p\big) \text{ and all } i, \text{ with } F \text{ the Frobenius automorphism}$$

$$\begin{aligned} Q_0\, h = {} & e_0 + (-1)^{p+1} r \sum_{m=0}^{p-1} s^m e_{p+m+1} + (-1)^p \Big(e_p + r\, e_{2p} + \sum_{m=1}^{p} s^m e_{p+m} \Big) \\ & + \sum_{j=1}^{p-1} (-1)^{pj} \Big[e_j + r\, s^{p-j} e_{2p} + r \sum_{m=0}^{p-j-1} s^m \big(e_{p+j+m} + (-1)^{p+1} e_{p+j+m+1} \big) \Big] \end{aligned}$$

$$\begin{aligned} Q_k\, h = {} & (-1)^{p(p-k)} \binom{p}{k} \Big(e_p + r\, e_{2p} + \sum_{m=1}^{p} s^m e_{p+m} \Big) + \sum_{j=k}^{p-1} (-1)^{p(j-k)} \binom{j}{k} \Big[e_j \\ & + r\, s^{p-j} e_{2p} + r \sum_{m=0}^{p-j-1} s^m \big(e_{p+j+m} + (-1)^{p+1} e_{p+j+m+1} \big) \Big] \quad \text{for } 0 < k < p \end{aligned}$$

$$Q_p\, h = e_p + r\, e_{2p} + \sum_{m=1}^{p} s^m e_{p+m}$$

where $r = h - p^2 + (-1)^p$, $s = p + (-1)^p$, and

$$\begin{aligned} e_n = {} & \sum_{m=n}^{p+1} (-1)^{(p+1)(m-n)} \binom{m}{n} Q_{m-1} \\ & + \sum_{m=n}^{2p} (-1)^{(p+1)(m-n)} \binom{m}{n} \sum_{\substack{i+j=m \\ 0 \le i,j \le p}} \sum_{\tau=1}^{p} w_{\tau+1}\, d_{i,\tau}\, Q_j \end{aligned}$$

the first summation for e_n being vacuous if $p+2 \le n \le 2p$, and being vacuous in its term $m = 0$ if $n = 0$.

Remark 1.8 The Dyer-Lashof algebra Γ has the structure of a twisted bialgebra over E^0. The "twists" are described by the commutation relations above. The product structure is encoded in the Adem relations. Certain Cartan formulas give rise to the coproduct structure.

In Section 4.2 below, we will present a proof for the commutation relations, in such a way that the same method applies to give the Cartan formulas: for each $0 \le k \le p$, $Q_k(xy)$ equals the expression on the right-hand side of the commutation relation for $Q_k h$, where $r = h - p^2 + (-1)^p$ and $s = p + (-1)^p$ as above, and

$$e_n = \sum_{m=n}^{2p} (-1)^{(p+1)(m-n)} \binom{m}{n} \sum_{\substack{i+j=m \\ 0 \le i,j \le p}} Q_i(x)\, Q_j(y)$$

1.3 Acknowledgements

I thank Paul Goerss, Charles Rezk, and Joel Specter for helpful discussions.

I thank my friends Tzu-Yu Liu and Meng Yu for their continued support, especially during me sketching Section 3 in their home in California.

2 Parameters in a modular equation

In this section, we discuss preliminaries needed for proving the main results. For some of the details, with examples, we refer the reader to [Zhu2015, Sections 2 and 3].

Given a formal group $\mathbb{G}_0$ over $\overline{\mathbb{F}}_p$ of height 2, let $\mathbb{G}$ be its universal deformation over the Lubin-Tate ring $\mathbb{W}\big(\overline{\mathbb{F}}_p\big)[\![h]\!]$. Let E be a Morava E-theory spectrum of height 2 at the prime p, such that $E^0 \cong \mathbb{W}\big(\overline{\mathbb{F}}_p\big)[\![h]\!]$ and $\operatorname{Spf} E^0\mathbb{CP}^\infty \cong \mathbb{G}$.

Recall from [Zhu2015, Section 2.1] that there are $\mathcal{P}_N$-*models* for the above data, constructed from the moduli of smooth elliptic curves, where $N > 3$ are integers prime to p. Specifically, each $\mathcal{P}_N$ is a moduli problem that encodes the choice of a point of exact order N and a nonvanishing one-form. It is represented by a scheme $\mathcal{M}_N$ over $\mathbb{Z}[1/N]$. Via the Serre-Tate theorem, the formal group of the representing elliptic curve is isomorphic to the universal deformation $\mathbb{G}$ of $\mathbb{G}_0$. Up to isomorphism, the E-theory is independent of the choice of a $\mathcal{P}_N$-model.

The purpose of choosing a $\mathcal{P}_N$-model is to enable explicit calculations for power operations in the E-theory. In particular, there are parameters from the moduli of elliptic curves that are both geometrically interesting and computationally convenient.

Recall from [Zhu2015, Section 3.1] that a total power operation ψ^p on E^0 corresponds to a deformation of p-power Frobenius $\Psi_N^{(p)}$ on the universal $\mathcal{P}_N$-curve [Rezk2009, Theorem B]. In particular, under this correspondence, we choose a pair of parameters h (as for E^0 above) and α for ψ^p as follows, which translate respectively to the *deformation* parameter T and the *norm* parameter $\mathbf{N}(\mathrm{X}(\mathrm{P}))$ for $[\Gamma_0(p)]$ at a supersingular point in [Katz-Mazur1985, Section 7.7].

The simultaneous moduli problem $\big(\mathcal{P}_N, [\Gamma_0(p)]\big)$ is represented by a scheme $\mathcal{M}_{N,\,p}$, which is finite and flat over $\mathcal{M}_N$ of degree $p+1$. Upon formal completion at the supersingular point corresponding to $\mathbb{G}_0$, the scheme $\mathcal{M}_{N,\,p}$ is isomorphic to the formal spectrum of the target ring of ψ^p [Strickland1998, Theorem 1.1].

Via a *dehomogenization* procedure, the parameters h and α are constructed from weakly holomorphic modular forms H (a factor of a Hasse invariant) and κ on $\Gamma_1(N)\times\Gamma_0(p)$ (see [Zhu2015, Proposition 2.8 and Examples 2.6 and 3.4]). Moreover, the *Atkin-Lehner involution* of $[\Gamma_0(p)]$ gives a new pair of parameters $\widetilde{h}$ and $\widetilde{\alpha}$ for ψ^p (cf. [Katz-Mazur1985, 11.3.1]). In fact, they are the images of h and α under ψ^p.

As a result of Lubin's isogeny construction in [Lubin1967, proof of Theorem 1.4], the parameter α plays a double role, which is important for our application. Algebraically, it is a norm by construction and is hence $\Gamma_0(p)$-invariant [Zhu2015, Construction 3.1 (ii)]. Geometrically, it defines the cotangent map to the isogeny $\Psi_N^{(p)}$ [Zhu2015, Remark 3.2]. In particular, this leads to the following.

Proposition 2.1 *Let $\mathcal{M}_N$ and $\mathcal{M}_{N,\,p}$ be the moduli schemes defined above. In a punctured formal neighborhood of the cusps $\overline{\mathcal{M}}_N - \mathcal{M}_N$, the scheme $\mathcal{M}_{N,\,p}$, viewed as a relative curve over $\mathcal{M}_N$, has an equation*

$$(\alpha - p)\big(\alpha + (-1)^p\big)^p = 0$$

Proof Choose the particular local coordinate in [Ando1995, Theorem 4] on the universal $\mathcal{P}_N$-curve. Let α be the norm parameter constructed from this coordinate. In particular, $\alpha \cdot \widetilde{\alpha} = (-1)^{p+1}p$.

In view of the geometric interpretation for α above and the transformation of bases for cotangent spaces in [Zhu2015, Remark 3.16], we see that the stated equation follows from the discussion in the first new paragraph on page Ka-23 of [Katz1973]—there

the $(p+1)$ roots of this equation are given (in Katz's notation, $\ell := p$ and $n := N$). Note that when $p = 2$, as a result of choice of local coordinates, the isogeny π in [Katz1973, Section 1.11] differs by a sign from the restriction of the isogeny $\Psi_N^{(p)}$ around the ramified cusp of $\Gamma_0(p)$. $\square$

3 Proof of Theorem 1.2

Choose a $\mathcal{P}_N$-model for $\mathbb{G}$. In the scheme $\mathcal{M}_{N,p}$ representing the simultaneous moduli problem $\big(\mathcal{P}_N, [\Gamma_0(p)]\big)$, there exists a supersingular point in characteristic p whose corresponding j-invariant lies in $\mathbb{F}_p \subset \mathbb{F}_{p^2}$ (see, e.g., [Cox2013, Theorem 14.18 and Proposition 14.15]). Let $j_0 \in \mathbb{Z}$ be a lift of this j-invariant. Consider a formal neighborhood U that contains this single supersingular point. Note that $U \cong \operatorname{Spf} A_1$ and that it is preserved under the Atkin-Lehner involution.

Define a modular function $h := j - j_0$, where $j(z) = q^{-1} + 744 + O(q)$ as usual. It then serves as a deformation parameter for A_0 and A_1. Let α be a norm parameter for A_1. Thus there exists a unique polynomial

$$w(h,\alpha) = \alpha^{p+1} + \sum_{i=0}^{p} w_i\, \alpha^i \tag{3.1}$$

with $w_i \in \mathbb{W}\big(\overline{\mathbb{F}}_p\big)[\![h]\!]$ such that $A_1 \cong A_0[\alpha]/\big(w(h,\alpha)\big)$. Write $\widetilde{h}$ and $\widetilde{\alpha}$ for the images of h and α under the Atkin-Lehner involution.

Given the geometric interpretation of $\widetilde{\alpha}$ in Section 2 and in view of the Hasse invariant as defined in [Katz-Mazur1985, 12.4.1], since the deformation parameter $h = j - j_0$, the modular function $\widetilde{\alpha}$ on $\Gamma_0(p)$ has a q-expansion

$$\widetilde{\alpha}(z) = \mu(q^{-1} + a_0) + O(q) = \mu\, q^{-1} + O(1)$$

for some unit $\mu \in \mathbb{W}\big(\overline{\mathbb{F}}_p\big)^\times \cap \mathbb{Z}$ and $a_0 \in \mathbb{Z}$ such that $a_0 \equiv 744 - j_0 \mod p$.

Thus for $2 \le i \le p$, there exist constants $\widetilde{w}_i \in p\mathbb{Z}$ such that

$$\widetilde{\alpha}^p + \widetilde{w}_p\, \widetilde{\alpha}^{p-1} + \cdots + \widetilde{w}_2\, \widetilde{\alpha} = \mu^p q^{-p} + O(1)$$

On the other hand, we have

$$\widetilde{h}(z) = j(pz) - j_0 = q^{-p} + O(1)$$

Comparing the two displays above, we then have

$$\widetilde{\alpha}^p + \widetilde{w}_p\, \widetilde{\alpha}^{p-1} + \cdots + \widetilde{w}_2\, \widetilde{\alpha} = \mu^p\, \widetilde{h} + K + O(q)$$

for some $K \in \mathbb{Z}$. Passing to the mod-p reduction of this identity, we see that $K \in p\mathbb{Z}$.

Therefore, by an abuse of notation, we can instead choose a deformation parameter h (and w_i in (3.1) accordingly) such that

$$\widetilde{\alpha}^p + \widetilde{w}_p\, \widetilde{\alpha}^{p-1} + \cdots + \widetilde{w}_2\, \widetilde{\alpha} = \widetilde{h} + O(q)$$

without changing the expressions for A_0 and A_1 (note that α and $\widetilde{\alpha}$ are both independent of the choice of h). From this we obtain

$$\widetilde{\alpha}^{p+1} + \widetilde{w}_p\, \widetilde{\alpha}^p + \cdots + \widetilde{w}_2\, \widetilde{\alpha}^2 = \widetilde{h}\, \widetilde{\alpha} + O(1)$$

In view of the expression (under the Atkin-Lehner involution) for A_1 as a free module over A_0 of rank $p+1$, and in view of the q-expansions for $\widetilde{h}$ and $\widetilde{\alpha}$, we see that the last term $O(1)$ above must be constant.

Applying the Atkin-Lehner involution to this polynomial relation between $\widetilde{h}$ and $\widetilde{\alpha}$, we then conclude that except for $i = 1$, the coefficients w_i in (3.1) are all constants, or more precisely, $w_i \in \mathbb{Z}$. It remains to determine their values, which follows from Proposition 2.1 by continuity of modular functions over the moduli scheme. □

4 Proof of Theorems 1.6 and 1.7

Theorem 1.6 (i) follows from [Strickland1998, Theorem 1.1]. We show the remaining parts in two steps.

4.1 The total power operation formula and the Adem relations

To compute $\psi^p(h)$, we follow the recipe illustrated in [Zhu2015, Example 3.4] and generalize [Zhu2015, proof of Proposition 6.4]. Since

$$\begin{aligned} w(h,\alpha) &= w_{p+1}\alpha^{p+1} + \cdots + w_1\alpha + w_0 \\ &= w_{p+1}\alpha^{p+1} + \cdots - h\,\alpha + \widetilde{\alpha}\,\alpha \end{aligned}$$

is zero in the target ring of ψ^p, we have

$$h = w_{p+1}\alpha^p + \cdots + w_2\,\alpha + \widetilde{\alpha}$$

where $w_{p+1}, \ldots, w_2$ are constants, i.e., they do not involve h, as computed in Theorem 1.6 (i). Applying the Atkin-Lehner involution to this identity, we then get

$$\psi^p(h) = \widetilde{h} = w_{p+1}\,\widetilde{\alpha}^p + \cdots + w_2\,\widetilde{\alpha} + \alpha$$

For $1 \leq \tau \leq p$, we need only express each $\widetilde{\alpha}^\tau$ as a polynomial in α of degree at most p with coefficients in E^0. The constant terms $d_{0,\tau}$ of these polynomials have been computed as d_τ in [Zhu2015, proof of Proposition 6.4]. The same method there applies to give the stated formulas for the higher coefficients $d_{i,\tau}$ with $1 \leq i \leq p$.

To derive the Adem relations, we generalize [Zhu2014, proof of Proposition 3.6 (iv)] (cf. [Zhu2015, proof of Proposition 6.4]). In view of the relation $\alpha \cdot \widetilde{\alpha} = w_0$, we have

$$\begin{aligned}
\psi^p\big(\psi^p(x)\big) &= \psi^p \sum_{j=0}^{p} Q_j(x)\,\alpha^j \\
&= \sum_{j=0}^{p} \psi^p\big(Q_j(x)\big)\,\psi^p(\alpha)^j \\
&= \sum_{j=0}^{p} \left(\sum_{i=0}^{p} Q_iQ_j(x)\,\alpha^i\right)\widetilde{\alpha}^j \\
&= \sum_{j=0}^{p} \left(\sum_{i=0}^{j} w_0^i\, Q_iQ_j(x)\,\widetilde{\alpha}^{j-i} + \sum_{i=j+1}^{p} w_0^j\, Q_iQ_j(x)\,\alpha^{i-j}\right) \\
&= \sum_{k=0}^{p} \alpha^k \left(\sum_{j=0}^{p}\sum_{i=0}^{j} w_0^i\, d_{k,j-i}\, Q_iQ_j(x) + \sum_{j=0}^{p-k} w_0^j\, Q_{k+j}Q_j(x)\right)
\end{aligned}$$

where $d_{k,0} = 0$ if $k > 0$. Write the expression in the last line above as $\sum_{k=0}^{p} \Psi_k(x)\,\alpha^k$. For $1 \leq k \leq p$, the vanishing of each Ψ_k then gives the stated relation for Q_kQ_0.

4.2 The commutation relations

To facilitate computations, we perform a change of variables

$$\beta \coloneqq \alpha + (-1)^p$$

We then have

$$\begin{aligned}
\psi^p(hx) &= \psi^p(h)\,\psi^p(x) \\
&= \sum_{i=0}^{p} Q_i(h)\,\alpha^i \sum_{j=0}^{p} Q_j(x)\,\alpha^j \\
&= \sum_{m=0}^{2p} \left(\sum_{\substack{i+j=m \\ 0\leq i,j\leq p}} Q_i(h)\,Q_j(x)\right)\alpha^m
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{m=0}^{2p} \Bigg(\sum_{\substack{i+j=m \\ 0\le i,j\le p}} Q_i(h)\,Q_j(x) \Bigg) \big(\beta + (-1)^{p+1}\big)^m \\
&= \sum_{m=0}^{2p} \Bigg(\sum_{\substack{i+j=m \\ 0\le i,j\le p}} Q_i(h)\,Q_j(x) \Bigg) \sum_{n=0}^{m} \binom{m}{n} \beta^n (-1)^{(p+1)(m-n)} \\
&= \sum_{n=0}^{2p} e_n\,\beta^n
\end{aligned}
$$

where

$$
e_n = \sum_{m=n}^{2p} (-1)^{(p+1)(m-n)} \binom{m}{n} \sum_{\substack{i+j=m \\ 0\le i,j\le p}} Q_i(h)\,Q_j(x)
$$

Formulas for the terms $Q_i(h)$ above are given by Theorem 1.6 (ii). Note that $Q_1(h)$ includes a term of 1.

We now reduce $\psi^p(hx)$ above modulo $w(h,\alpha)$, by first rewriting the latter as a polynomial in β:

$$
\begin{aligned}
w(h,\alpha) &= (\alpha - p)\big(\alpha + (-1)^p\big)^p - \big(h - p^2 + (-1)^p\big)\alpha \\
&= \big(\beta + (-1)^{p+1} - p\big)\beta^p - \big(h - p^2 + (-1)^p\big)\big(\beta + (-1)^{p+1}\big) \\
&= \beta^{p+1} + v_p\,\beta^p + v_1\,\beta + v_0
\end{aligned}
$$

where

$$
v_p = (-1)^{p+1} - p, \quad v_1 = -\big(h - p^2 + (-1)^p\big), \quad \text{and} \quad v_0 = (-1)^{p+1} v_1
$$

Performing long division of $\psi^p(hx)$ by $w(h,\alpha)$ with respect to β, we get

$$
\psi^p(hx) \equiv \sum_{j=0}^{p} f_j\,\beta^j \mod w(h,\alpha)
$$

where

$$
f_j = \begin{cases}
e_p - v_1 e_{2p} + v_p \displaystyle\sum_{m=0}^{p-1} (-1)^{m+1} e_{p+1+m}\, v_p^m & j = p \\
e_j + v_0 \displaystyle\sum_{m=0}^{p-j-1} (-1)^{m+1} e_{p+j+1+m}\, v_p^m + v_1 \displaystyle\sum_{m=0}^{p-j} (-1)^{m+1} e_{p+j+m}\, v_p^m & 0 < j < p \\
e_0 + v_0 \displaystyle\sum_{m=0}^{p-1} (-1)^{m+1} e_{p+1+m}\, v_p^m & j = 0
\end{cases}
$$

Thus we can rewrite

$$\begin{aligned}\psi^p(hx) &= \sum_{j=0}^{p} f_j \left(\alpha + (-1)^p\right)^j \\ &= \sum_{j=0}^{p} f_j \sum_{i=0}^{j} \binom{j}{i} \alpha^i (-1)^{p(j-i)} \\ &= \sum_{i=0}^{p} \left[\sum_{j=i}^{p} (-1)^{p(j-i)} \binom{j}{i} f_j \right] \alpha^i\end{aligned}$$

On the other hand, $\psi^p(hx) = \sum_{i=0}^{p} Q_i(hx)\,\alpha^i$. Comparing this to the last expression for $\psi^p(hx)$ above, term by term, we obtain the commutation relations as stated. $\square$

References

[Ahlgren2003] Scott Ahlgren, *The theta-operator and the divisors of modular forms on genus zero subgroups*, Math. Res. Lett. **10** (2003), no. 6, 787–798. MR2024734(2004m:11059)

[Ando1995] Matthew Ando, *Isogenies of formal group laws and power operations in the cohomology theories E_n*, Duke Math. J. **79** (1995), no. 2, 423–485. MR1344767(97a:55006)

[Ando-Hopkins-Strickland2004] Matthew Ando, Michael J. Hopkins, and Neil P. Strickland, *The sigma orientation is an H_∞ map*, Amer. J. Math. **126** (2004), no. 2, 247–334. MR2045503(2005d:55009)

[Bruinier-Kohnen-Ono2004] Jan H. Bruinier, Winfried Kohnen, and Ken Ono, *The arithmetic of the values of modular functions and the divisors of modular forms*, Compos. Math. **140** (2004), no. 3, 552–566. MR2041768(2005h:11083)

[Choi2006] D. Choi, *On values of a modular form on $\Gamma_0(N)$*, Acta Arith. **121** (2006), no. 4, 299–311. MR2224397(2006m:11051)

[Cox2013] David A. Cox, *Primes of the form $x^2 + ny^2$*, second ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013, Fermat, class field theory, and complex multiplication. MR3236783

[Katz1973] Nicholas M. Katz, *p-adic properties of modular schemes and modular forms*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 69–190. Lecture Notes in Mathematics, Vol. 350. MR0447119(56 #5434)

[Katz-Mazur1985] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985. MR772569(86i:11024)

[Lubin1967] Jonathan Lubin, *Finite subgroups and isogenies of one-parameter formal Lie groups*, Ann. of Math. (2) **85** (1967), 296–302. MR0209287(35 #189)

[Lubin-Serre-Tate1964] J. Lubin, J.-P. Serre, and J. Tate, *Elliptic curves and formal groups*, available at http://www.ma.utexas.edu/users/voloch/lst.html.

[Lubin-Tate1966] Jonathan Lubin and John Tate, *Formal moduli for one-parameter formal Lie groups*, Bull. Soc. Math. France **94** (1966), 49–59. MR0238854(39 #214)

[Milne2012] J.S. Milne, *Modular functions and modular forms*, available at http://www.jmilne.org/math/.

[Quillen1969] Daniel Quillen, *On the formal group laws of unoriented and complex cobordism theory*, Bull. Amer. Math. Soc. **75** (1969), 1293–1298. MR0253350(40 #6565)

[Rezk2008] Charles Rezk, *Power operations for Morava E-theory of height 2 at the prime 2*. arXiv:0812.1320

[Rezk2009] Charles Rezk, *The congruence criterion for power operations in Morava E-theory*, Homology, Homotopy Appl. **11** (2009), no. 2, 327–379. MR2591924(2011e:55021)

[Rezk2012] Charles Rezk, *Modular isogeny complexes*, Algebr. Geom. Topol. **12** (2012), no. 3, 1373–1403. MR2966690

[Strickland1997] Neil P. Strickland, *Finite subgroups of formal groups*, J. Pure Appl. Algebra **121** (1997), no. 2, 161–208. MR1473889(98k:14065)

[Strickland1998] N. P. Strickland, *Morava E-theory of symmetric groups*, Topology **37** (1998), no. 4, 757–779. MR1607736(99e:55008)

[Zhu2014] Yifei Zhu, *The power operation structure on Morava E-theory of height 2 at the prime 3*, Algebr. Geom. Topol. **14** (2014), no. 2, 953–977. MR3160608

[Zhu2015] Yifei Zhu, *The Hecke algebra action on Morava E-theory of height 2*. arXiv:1505.06377

Department of Mathematics, Northwestern University, Evanston, IL 60208, USA

zyf@math.northwestern.edu